Evaluation of Performance Characteristics of Polynomial based and Lattice based NRTU Cryptosystem

Rakesh Nayak[1], Jayaram Pradhan[2], and C.V. Sastry[3]
Sri Vasavi Engineering College,Department of IT,
Tadepalligudem,Andhra Pradesh, India
nayakrakesh8@gmail.com
Behrampur University,Department of Computer Sciences,
Behrampur, Odisha, India
jayarampradhan@hotmail.com
Sreenidhi Institute of Science and Technology, School of Computer Science and informatics,
Hyderabad, Andhra Pradesh, India
cvsastry40@yahoo.co.in

Abstract: **In order to achieve the security for the e-business application, generally, the organizations follow the cryptographic methods. The two widely accepted and used cryptographic methods are symmetric and asymmetric. The DES ideally belongs to the category of symmetric key cryptosystem and RSA, NTRU[3] belongs to the category of asymmetric key cryptosystem. NTRU (Nth degree truncated polynomial ring units) is a collection of mathematical algorithms based on manipulating lists of very small integers. NTRU is the first secure public key cryptosystem not based on factorization or discrete logarithmic problems. The keys are generated by having small potent polynomials from the ring of truncated polynomials. NTRU can also be implemented using matrices instead of polynomials [4, 5]. We proceed with the encryption and decryption of the plain text required by implementing the algorithms of both the approaches of NTRU cryptosystems. It is already shown that the matrix approach is algorithmically better than the polynomial approach of NTRU cryptosystem [5]. We propose and test both the methods for variable sized text files, using polynomial and matrix cryptosystems. This paper presents the comparative study of polynomial NTRU and matrix NTRU algorithms for variable sized text files as input. The final results were observed using Mathematica5.1, analyzed and compared so as to identify which method is appropriate to the business needs.**

KeyWords: **Data Security, Encryption, Decryption, Polynomial, Matrix.**

I. Introduction

The two major reasons which made Public-Key cryptographic algorithms more reliable are the areas of greater confidentiality, ease of key generation and authentication. These algorithms are based on mathematical calculations rather than substitutions and permutations like the symmetric cryptosystems. Further these algorithms use two keys in contrast to symmetric algorithms which uses only one key. Public-Key algorithms rely on one key for encryption and a different but related unique key for decryption.It is computationally infeasible to determine the decryption key given only the knowledge of cryptographic algorithm and the encryption key. The two keys in Public-Key Cryptographic algorithms are referred as public key and private key. Invariably the private key is kept secret and is only known to the user that holds it.In the subsequent sections, we present the implementations of polynomial based NTRU and lattice based NTRU systems for different text files and finally compare the computational running times to find the suitable method for the business applications.

II. NTRU with Polynomial Approach

The NTRU encryption system and the related signature scheme are both built on polynomial algebra. The basic objects are truncated polynomials [3, 7] in the ring $R = Z[x]/(Z^N - 1)$ and the basic tool is the reduction of polynomials with respect to two relatively prime moduli. The security of the systems is based on the difficulty of finding a "short" factorization for such polynomials. This latter problem is equivalent to finding a short vector in a certain $2N$ dimensional lattice, a commonly known and also widely studied hard problem. NTRU polynomials $a(x)$ are frequently reduced modulo p and q, the small and large moduli. The large modulus q is an integer, and reduction of $a(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} \bmod q$ means just reduction of each a_i modulo q. The small modulus *p* can also be an integer. It is required that *p* and *q* are relatively prime: $\gcd(p, q) = 1$.The main objects in the systems are "small" polynomials; i.e. polynomials with small coefficients, or polynomials with a small norm (Euclidean length of the coefficientvector). The public key h is defined by an equation $f * h = pg(\bmod q)$, where f and g are small polynomials. The polynomial f should always have inverses modulo p and q [3], $f * fp \equiv 1(\bmod p)$ and $f * fq \equiv 1(\bmod q)$ .Moreover, the parameters N , p and q are also public, and can be used as common domain parameters for all users. Polynomials f and g are private to the key owner. The polynomial g is needed only in key generation.

Bob chooses two small polynomials f and g in the ring of truncated polynomials and keeps f and g private. He then computes fp and fq , where p and q are relatively prime to each other. He computes $h = pfq * g (\bmod q)$, which becomes the public key for Bob and the pair of polynomials f and fp forms his private key pair. The message is also represented in the form of a truncated polynomial. Let it be m .

Alice encrypts using the public key of Bob i,e, h as $e = h * r + m (\bmod q)$,where r is a random polynomial basically used to obscure the message. This encrypted message may be sent in a public not secure channel. Bob decrypts the encrypted message using his private key pair by performing the following operations:

$a = f * e (\bmod q)$

$b = a (\bmod p)$

$c = fp * b (\bmod p)$, c is the original message,

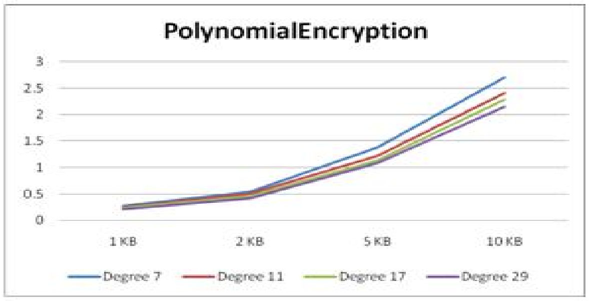
As $c = fp * [f * (pfq * g * r + m)](\bmod q)(\bmod p) = m$ using the identities $f * fp \equiv 1 (\bmod p)$ and $f * fq \equiv 1 (\bmod q)$.

A. NTRU Encryption

Alice has a message to transmit to Bob. Alice first puts the message in the form of a polynomial m whose coefficients are chosen modulo p , say , between $-p/2$ and $p/2$ .Next Alice randomly chooses another small polynomial r . This is the binding value which is used to obscure the message. She uses the message m, randomly chosen polynomial r , and Bob's public key h to compute the polynomial $e = h * r + m (\bmod q)$. The polynomial e is the encrypted message which Alice sends to Bob.

TableI.I. Polynomial Encryption

File Size	Encryption			
	Polynomial with			
	Degree 7	Degree 11	Degree 17	Degree 29
1 KB	0.271600000000000	0.249800000000000	0.230799999999999	0.215000000000009
2 KB	0.542800000000000	0.502599999999999	0.455399999999997	0.424600000000009
5 KB	1.369800000000000	1.219999999999990	1.132399999999990	1.076400000000010
10 KB	2.699000000000000	2.411800000000000	2.283600000000000	2.143199999999990



A. NTRU Decryption

Bob has received Alice's encrypted message e and Bob wants to decrypt it. He begins by using the private polynomial f to compute the polynomial $a = f * e (\bmod q)$ and chooses the coefficients of a to lie between $-q/2$ and $q/2$. In general Bob will choose the coefficients of a to lie in an interval of length q .The specific interval depends on the form of the small polynomials. It is very important that he does this before performing the next step. He next computes the polynomial $b = a (\bmod p)$. That is, he reduces each of the coefficients of a modulo p . Finally he uses the other private polynomial fp to compute $c = fp * b (\bmod p)$. The polynomial c will be Alice's original message m. The decryption procedure is executed by the following three steps :

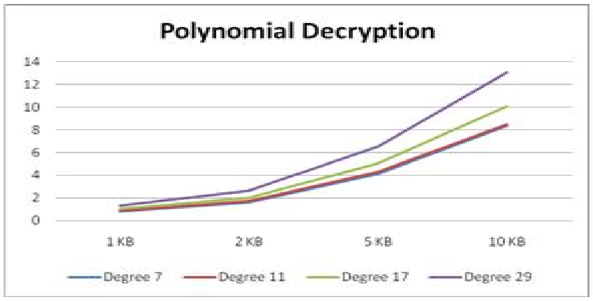
$a = f * e (\bmod q)$

$b = a (\bmod p)$

$c = fp * b (\bmod p)$

TableI.II. Polynomial Decryption

File Size	Decryption			
	Polynomial with			
	Degree 7	Degree 11	Degree 17	Degree 29
1 KB	0.836399999999999	0.855000000000000	1.017200000000000	1.310799999999990
2 KB	1.650400000000000	1.712999999999990	2.012199999999990	2.608199999999990
5 KB	4.183800000000000	4.274600000000000	5.010800000000000	6.498799999999990
10 KB	8.393000000000000	8.479999999999990	10.058999999999999900	13.041600000000000000



DOI: 01.IJNS.03.01. 46

III. NTRU with Lattice Approach

Let R^m be a m-dimensional Euclidean space . A lattice [4] in R^m is a set of integers combinations $L(b_1,b_2,...,b_n)=\{\sum_{i=1}^{n} x_i b_i : x_i \in Z \text{ for } 1 \le i \le n\}$ for n linearly independent $b_1,b_2,...,b_n$ in R^m $(m \ge n)$. The integers' m and n are called rank and dimension of the lattice respectively.

A basis can be represented by the matrix $B=[b_1,b_2,...,b_n] \in R^{mxn}$ having the basis $l(B)=\{Bx : x \in Z^n\}$, where Bx is the usual matrix multiplication. Each b_i represents a column of a matrix. In matrix notation $Z^m = l(I)$, where $I \in Z^{nxn}$ is the n-dimensional identity matrix i.e., n x n square matrix with 1's on the diagonals and 0's everywhere. When $n = m$ i.e., the number of basis vectors equals the number of coordinates, we say that $l(B)$ is of full rank or full dimensional. Equivalently, lattice $l(B) \in R^n$ is full rank if and only if the linear span of the basis vector $(B)=\{Bx : x \in R^n\}$ equals the entire space R^n.

So B, an n x n matrix defined as

$$B = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{bmatrix}$$

This represents some points in a n X n space of real numbers. Let p be an integer. Then we define B (mod p) as

$$a = B(\text{mod } p) = \begin{bmatrix} b_{11}(\text{mod } p) & \cdots & b_{1n}(\text{mod } p) \\ \vdots & \ddots & \vdots \\ b_{n1}(\text{mod } p) & \cdots & b_{nn}(\text{mod } p) \end{bmatrix}$$

This represents some points in a n x n space of positive integers. A matrix and congruence with the same modulus may be added, subtracted, and multiplied just as is done with matrix operations[4,5].

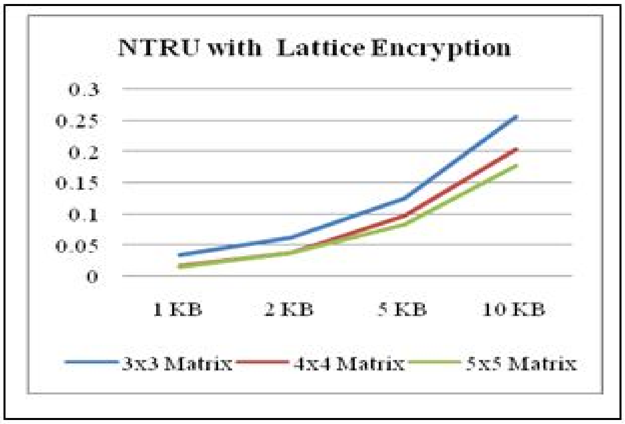
Bob creates a public/private key pair. He first randomly chooses two matrices X and Y, where matrix X should be an invertible matrix (modulus p and q). He keeps the matrices X and Y private, since anyone who knows either one of them will be able to decrypt messages sent to Bob. He compute the inverse of $X(\text{mod } q)$ and the inverse of $X(\text{mod } p)$. Thus he computes matrix Xq and Xp which satisfies $X * Xp \equiv I(\text{mod } p)$ and $X * Xq \equiv I(\text{mod } q)$. Bob can ensure the existence of inverse of matrix X by checking X is non-singular and X is invertible mod p (i.e. $\det[X](\text{mod } p) \ne 0$). Otherwise he needs to go back and choose another matrix X. Now Bob computes the product $H = pXq * Y(\text{mod } q)$. His private key is the pair of matrices X and Xp and his public key is the matrix H.

A. NTRU with Lattice Encryption

Alice wants to send a message to user Bob using his public key H. Alice first puts her message in the form of a binary matrix M, (which is a matrix of same order as X and Y) whose elements are chosen mod p. Next, A randomly chooses another matrix R of the same order as X. This is the "blinding value", which is used to obscure the message (similar to the way that the ElGamal algorithm uses a onetime random value when encrypting). To send message M, Alice chooses a random matrix R (which is of same order as matrix X), and Bob's public key H to compute the matrix $E = [H * R + M](\text{mod } q)$. The matrix E is the encrypted message which Alice sends to Bob.

Table I.III. Lattice Encryption

Text Size	Encryption		
	3x3 Matrix	4x4 Matrix	5x5 Matrix
1 KB	0.034200000000000	0.015999999999997	0.015400000000000
2 KB	0.062200000000001	0.037400000000002	0.037600000000009
5 KB	0.124800000000000	0.096199999999999	0.084199999999998
10 KB	0.255800000000002	0.202999999999985	0.177400000000011



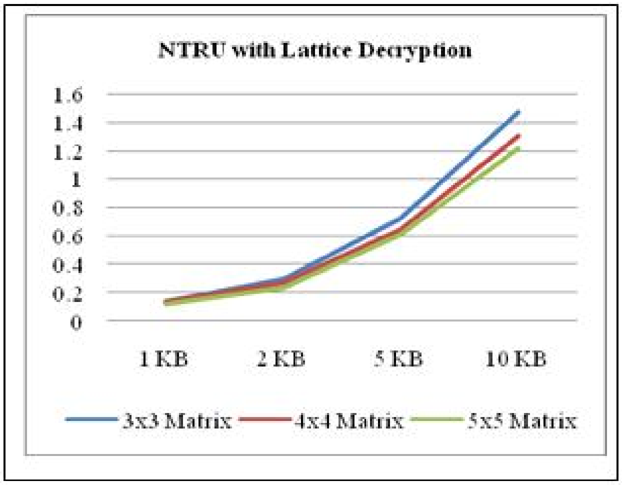
B. NTRU with Lattice Decryption

Now Bob has received Alice's encrypted message E and he decrypts it. He begins by using his private matrix X to compute the matrix. $A = X * E(\text{mod } q)$. Bob next computes the matrix $B = A(\text{mod } p)$. Finally Bob uses his other private matrix Xp to compute $C = Xp * B(\text{mod } p)$. The matrix C will be Alice's original message M.

DOI: 01.IJNS.03.01.46

TABLE 1.IV. LATTICE DECRYPTION

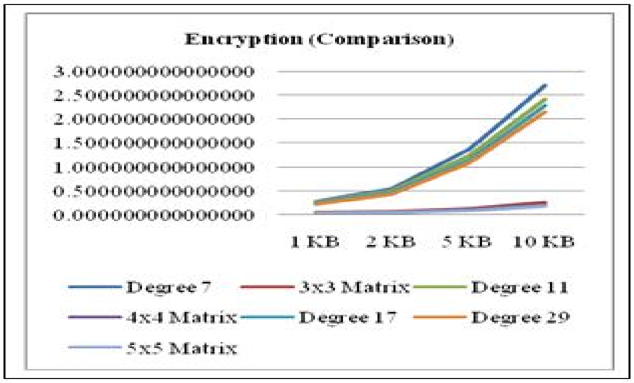
Text Size	Decryption		
	3x3 Matrix	4x4 Matrix	5x5 Matrix
1 KB	0.140600000000000	0.137200000000001	0.124799999999993
2 KB	0.296400000000000	0.265200000000004	0.239999999999997
5 KB	0.729999999999995	0.651800000000003	0.611399999999991
10 KB	1.472799999999990	1.307399999999990	1.216600000000000

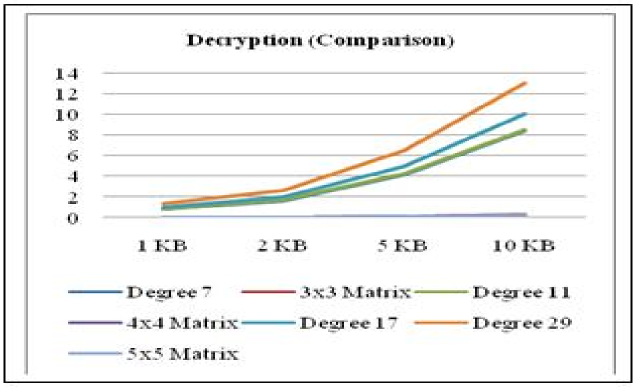


IV. COMPARISON

NTRU cryptosystem is a technique to encrypt/decrypt block of data. It uses Truncated Polynomials for encryption and decryption. In this paper we have used matrices in place of truncated polynomials. We have compared 7-bit polynomial with 3x3 matrix (9-bit), 11-bit polynomial with 4x4 matrix(16-bit) and polynomial with degree 17 and 29 with 5x5 matrix (25-bit). Although the matrix approach has more bits compared to that of corresponding polynomial approach, it is observed that encryption/ decryption times are faster.

The following graphs clearly show that the lattice approach of NTRU is faster than that of polynomial approach of NTRU cryptosystem.





V. CONCLUSION

In this paper it is shown that the lattice approach of NTRU cryptosystem is computationally faster than that of polynomial approach. Hence this method is suitable to send large messages. Also it is more secure since matrices are non commutative. There is no easy method to know whether a polynomial is invertible or not. We can use this method as a matrix is invertible only when it's determinant is found. With an improved algorithm for matrix multiplication these results can further be optimized. We can choose different types of lattices to further improve the complexity.

REFERENCES

[1]. Whitefield Diffie, Martin E Hellman "New directions in cryptography" IEEE Information theory, June 23- 25, 1975 and IEEE International Symposium on Information theory, Sweden, June21-24, 1976.

[2]. Huffman "A method for the construction of minimum redundancy codes" Proc. IRE, vol. 40, pp. 1098–1101, Sept. 1952.

[3]. Joffrey Hoffstein , Jill Pipher , Joseph H Silverman"NTRU-A Ring based public key cryptosystem" Lecture notes in Computer Science, Springer-Verlag, Berlin 1433(1998),267-288.

[4]. Rakesh Nayak, C.V.Sastry, Jayaram Pradhan, "A matrix formulation for NTRU cryptosystem.", Proceedings 16th IEEE, International Conference on Networks (ICON-2008), New Delhi, from date 12th-14th Dec'08.

[5]. Rakesh Nayak, C.V.Sastry, Jayaram Pradhan," Algorithmic Comparison between Polynomial Base and Matrix Base NTRU Cryptosystem "International Journal of computer and Network Security,(IJCNS) Vol. 2, No. 7, July 2010.

[6]. Jeffry Hoffstein, Jill Pipher and Joseph H. Silverman "NTRU: A High Speed Public Key Cryptosystem", PrePrint Presented At He Hump Session Of Euro Crypt 96,1996.

[7]. J. Hoffstein, D. Lieman, J. Silverman" Polynomial Rings and Efficient Public Key Authentication", Proceeding of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99), M. Blum and C.H. Lee, eds., City University of Hong Kong Press,1999.

[8]. E.Horowitz, S.Sahani & S.Rajasekharan "Fundamental of Computer Algorithm",Galgotia,1998.

[9]. I.N. Herstein, Topics in Algebra, John Wiley & Sons, second edition, New York, (1975).

[10]. NTRU Cryptosystem, Technical Reports 2002 available at http://www.ntru.comWikipedia , the free encyclopedia " NTRU Cryptosystems Inc.,"

DOI: 01.IJNS.03.01.46